

2.3.6 Electronic Payment Systems

*Ahmad-Reza Sadeghi*²⁷⁷, *Markus Schneider*²⁷⁸

Abstract: With the development of digital rights management systems, new commercial applications for the trade with digital goods will be introduced, and new information services will be provided. As digital goods or services can be delivered over networks, it is also desired that they can immediately be paid electronically. Thus, it is assumed that the trade with digital goods stimulates the deployment of electronic payment systems. Furthermore, new commercial models make new demands on specialized payment systems, e.g., low-value payments should be supported in an economically reasonable way. Meanwhile, there exists a large body of literature on electronic payment system. In this paper, we give a survey of these systems. We point out the requirements they should fulfill and present briefly the basic principles for different categories of payment systems, and consider a few candidates.

I Introduction

Since the overcoming of barter in the history of mankind, trade usually involves the exchange of goods and equivalent abstract values, such as money. Over years, many variants have been introduced of how to pay and thereby handing over monetary values in commercial relationships, e.g., cash as coins, cash as banknotes, cheques, or early paper-based credit card payments²⁷⁹. This was before electronic payment systems.

With the dispersal of digitalization and the availability of communication networks, a large number of electronic payment systems have been proposed and developed which provide new means for the representation of values. Loosely spoken, in electronic payment systems monetary values are transferred electronically between a payer and a receiver. Note that exchange of values among financial institutions for the purpose of clearing is also carried-out electronically. However, clearing systems are outside our considerations here.

There were many reasons — technical and economical ones — driving the tremendous effort done in the area of electronic payment systems. Here, we restrict our considerations exclusively to technical aspects. Among them, two important reasons are:

- Security aspects: Traditional means for payment show various security problems such as counterfeit banknotes. One of the main goals of electronic payment systems was to achieve a higher level of security as offered by traditional systems, even if electronic payment systems introduce new kinds of threats.
- Commerce over communication networks: In case of commercial relationships where involved parties are connected over communication networks, traditional means for payment cannot be used anymore which assume physical

²⁷⁷ Saarland University, Computer Science.

²⁷⁸ Fraunhofer Gesellschaft, Institute for Secure Telecooperation.

²⁷⁹ See: Davies (1996).

contact. Thus, electronic business processes of geographically distant parties require that monetary values can be transferred over networks.

In the early years of doing business electronically up to now, most popular electronic shops were focusing predominantly on the exchange of physical goods, such as books or CDs. As experience has shown in this context, buyers have mainly used conventional payment systems either electronic or traditional, e.g., credit cards or bank transfer after delivery of goods. User behaviour varies in international context. Unfortunately, often more modern electronic payment systems that have been developed and tested in several field trials in the last years were not successful, and thus were not used in real life applications. There are many reasons having caused this²⁸⁰. For customers there was often no obvious reason to get used to new and complicated payment systems when they were able to manage the needs with their conventional payment systems. Furthermore, customers did not use specific payment systems which were not provided by a large merchant base. On the other hand, the low number of customers did not stimulate merchants to provide new electronic payment systems.

The growing market for digital goods supported by the availability of digital rights management systems may change some conditions regarding electronic payment systems. Digital goods allow that all phases of a typical business process from *search* to *delivery* are carried out electronically. Thus, it is reasonable for those business processes to also involve the electronic exchange of monetary values. This can be done immediately before or after delivery. In this context, electronic payment systems have to be usable for transferring value over networks such as the Internet. Furthermore, especially in the trade with digital goods, one may expect certain commercial relationships that require payments of low values, e.g., in the range from a few Cents to a few Euros. As an example for such a case consider a merchant that sells small-sized digital products like newspaper articles. In another example, a commercial model might be based on metered usage of digital products in a digital rights management system where a consumer has to pay low values for specific activities. Note that in general, electronic payment systems do not guarantee the delivery of purchased goods. Solutions for *fair exchange* are not the subject of this paper.

In the following, we will give an overview of electronic payment systems. Our aim is not to cover all electronic payment systems that have been proposed in the last 20 years. Instead, our intent is to summarize the most important requirements for electronic payment systems and to categorize them. Furthermore, we explain the basic concepts and principles which are applied in these categories in a rather abstract way, i.e., without going into the details of specific electronic payment systems. Nevertheless, we will mention some concrete proposals for each category. Finally, we will shortly present some current sample systems which are used in practice.²⁸¹

²⁸⁰ See: Yung (2000).

²⁸¹ Other work providing either short surveys or more comprehensive treatments of electronic payment systems can be found in: Asokan, Janson, Steiner, Waidner

II Models

In a commercial context, payment always involves a *payer* P spending money and a *merchant* M who receives the money. P and M may have accounts at distinct banks, B_P and B_M , respectively.

As for traditional payment systems, electronic payments can be carried out in many ways. Here, we consider the basic types of payment systems: cash-like, cheque or credit card, remittance, and debit order. The way how the exchange of real money among the banks is initiated in these systems varies as can be seen in Figure 1:

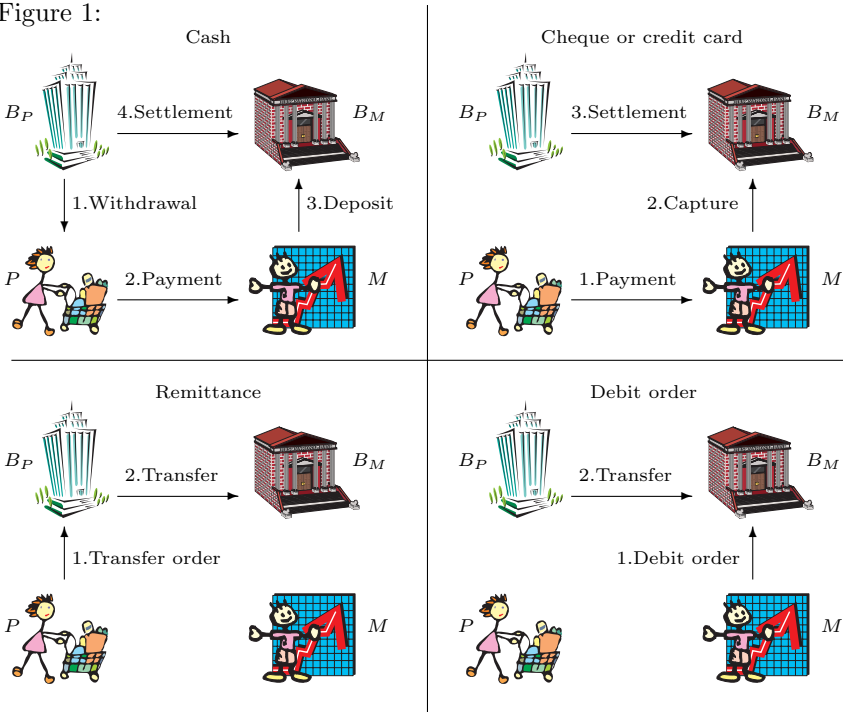


Fig. 1. Types of Payment Systems

In *cash* systems, P obtains electronic cash in the *withdrawal* phase from B_P . For this cash, B_P debits a corresponding amount of money from P 's account. Then P can start his purchases where she pays with this cash. In the *payment* phase, the cash is transferred to M . In the *deposit* phase M forwards the cash to his bank B_M that initiates the *settlement* phase in which real money is exchanged from B_P to M 's account at B_M .

Regarding the sequence of phases, *cheque* and *credit card* payment belong to the same category of payment systems. Both start with the *payment* phase in which

(1996/1997/2000); O'Mahony, Peirce, Tewari (1997); Pilioura (1998); Pfizmann, Waidner (1996); Schmidt, Schunter, Weber (1998); Jakobsson, MRaihi, Tsiounis, Yung (1999); Abrazhevich (2001a).

P sends a filled-in electronic form to M . In the *capture* phase, M hands this to B_M who receives the money from B_P in the *settlement* phase.

Both types above are *direct* payments since there is a direct interaction between the payer and the merchant. Another category of systems deals with *indirect* payments. In these, only one party, either P or M , is involved in the payment. *Remittance* and *debit order* systems belong to the category of *indirect* payments. Although, they are often used in electronic business relationships, we will not consider them here in detail. These systems are mainly based on financial networks and usually do not involve open networks such as the Internet. Here, our interest is more in modern payment systems that can be used over open networks.

Debit order systems may be suited for subscription models at large merchants. In such systems, the merchant periodically requests the payer's bank for the payment, e.g., monthly or yearly. But subscription models will only be deployed in such business models in which customers rather regularly request services or products, e.g., newspaper articles.

These basic payment models are surely helpful when classifying proposed electronic payment systems. However, there are also payment systems whose underlying model cannot be fully assigned to one of these basic models we have considered here.

In general, the choice of a payment system best suited for a specific commercial relationship may depend on various conditions, e.g., concrete systems supported by the merchant, trust in payment systems or organizations behind them, privacy requirements, additional costs.²⁸²

III Requirements for Payment Systems

In this section, we consider the main security and privacy requirements for electronic payment systems in general. Note that not all of these requirements are necessarily relevant and have to be fulfilled for all different types of payment systems which will be presented later. Requirements for systems usually vary according to their specific features and the underlying trust assumptions. In fact, there are also other important requirements for electronic payment systems, e.g., usability, acceptability, scalability, interoperability, availability²⁸³. However, due to space limitations, these will not be considered here.

III.1 Fraud Prevention

Similar to traditional payment systems, security aspects are of central interest for electronic payment systems. Thus, the prevention of fraud and theft resulting in monetary loss for honest parties and profit for malicious parties is an important requirement. Obviously, electronic payment systems have to cope at least with

²⁸² For more details see: Abrazhevich (2001b/c).

²⁸³ See: Abrazhevich (2001b/c); Schmidt, Schunter, Weber (1998).

the same threats as physical payment systems do; there is potential of minting and printing counterfeit money, forging cheques, stealing credit card numbers, and many more things adversaries might try. Electronic payment systems should require that the — usually contradicting — interests of all involved parties are protected.

One of the main security requirements is *unforgeability* of monetary value. This concerns various aspects:

- creation of new monetary value,
- modification of monetary value,
- overspending.

The first aspect deals with *data origin authentication* of digital monetary values. Since malicious parties cannot be prevented from attempting to forge, this guarantees that maliciously created monetary values can be detected. Another aspect considers the *integrity* of data which represent monetary values. It is necessary that amount modifications can be detected, e.g., changing the amount of an electronic cheque or electronic cash a posteriori. The next aspect of unforgeability stems from the fact that digital monetary values can be copied very easily where the original and copies are indistinguishable. Thus, electronic payment systems require *protection against overspending*. There are different strategies to do this: *overspending detection* where overspent copies are immediately detected at the moment of spending it, or *overspender tracing* where the overspending party can be identified afterwards.

Parties are also interested that no payments are actually initiated without their consent. This is tackled by the requirement of *authorization*. This involves aspects as to allow access to installations exclusively to their owners, and for parties / systems to act according to other parties' instructions only if these are authentic, or even better, if they are non-repudiable.

III.2 Confidentiality

Electronic payment systems should offer at least as much confidentiality as traditional payment systems currently do. The goal of this requirement is that payment data should not be exploitable in order to obtain more precise or more comprehensive information about involved entities, e.g., payer profiles. Thus, confidentiality properties of electronic payment systems can be distinguished regarding which information they reveal to which parties. Confidentiality of payment information against other parties can be achieved by encrypting communication which is no specific property of payment systems. Note that confidentiality in electronic payment systems cannot prevent information flows which may happen outside an electronic payment system among involved parties, e.g., by observing communication networks, or revealing data in further commercial interactions.

Preventing undesired linking of specific information to identities can be achieved by anonymization techniques. Electronic payment systems can have different goals regarding the realization of anonymity, i.e., who should be anonymous

from whom. Note that confidentiality is not necessarily achieved by only using anonymization techniques. Obviously, anonymity is only possible if the set of people which are potential candidates is large enough. Technically, one can also distinguish among different types of anonymity. In a system in which a party does not obtain another party's identity, it may still be possible to link several activities (e.g., payments) stemming from the same party. In systems providing *unlinkability* no relations among different actions in the electronic payment system can be established, e.g., to link payments of the same payer.

Most proposals focus on privacy concerns of payers when banks get insight at which merchants they buy²⁸⁴. From such information, banks may come to further conclusions which the payer might want to prevent; e.g., when a bank gets aware that a payer often buys at pharmacies it may draw conclusions about the general health of the payer. In this context, electronic payment systems with payer anonymity against the bank are of interest. This means that monetary values obtained by the merchant from the payer and then forwarded to the bank should not reveal the payer's identity. There are also some proposals dealing with recipient anonymity²⁸⁵.

In an electronic payment system in which a party is completely anonymous against other parties, there is the risk that anonymity may be misused, e.g., in case of money laundering or blackmailing²⁸⁶. Thus, there are proposals in which anonymity can be revoked under certain circumstances, such as *escrowed payment systems*.

III.3 Fault Tolerance

There is a requirement to protect parties from financial losses in case of system crashes and network failures. Parties have a strong interest to be safeguarded against financial loss because of events which are beyond their control. Thus, electronic payment systems require that parties can be reimbursed for monetary value they have lost. Obviously, these solutions have to take into consideration parties that falsely claim a loss and maliciously try to achieve a profit.

Furthermore, electronic payment systems have to follow the transaction concept in order to guarantee that they always are in a consistent state. This means that a payment protocol is atomic, i.e., it is either executed completely or not at all.

IV Properties of Payment Systems

In this section, we present some of the main properties of electronic payment systems that should be considered when comparing systems or selecting a system for a special purpose or application.

²⁸⁴ See: Chaum (1983/1986); Chaum, Fiat, Naor (1990).

²⁸⁵ See: Chaum (1989).

²⁸⁶ See: Sander, Ta-Shma (1999); Solms, Naccache (1992).

IV.1 Small- and Low-Value Payments

Small- and low-value payments require low transaction costs. If a product's price, e.g., for a web page, a single music file or a newspaper article, is in the range of only some Cents or even smaller, then the overhead costs for a credit card payment would be a multiple of the costs for a product (e.g., for sample costs see Jakobsson, MRaihi, Tsiounis, Yung/ Micali, Rivest²⁸⁷). Sometimes, even many small amounts have to be paid to the same merchant for different products where it is not possible to pay the sum of all these amounts at once, e.g., for telephone calls. Thus, efficient and low-cost processing of low-value payments requires specific electronic payment systems. Such micropayment systems are assumed to be of considerable importance for commerce focusing on digital goods. Since high processing costs of some systems also stem — among other reasons — from their high computational effort (e.g., because of digital signature generation), application of efficient primitives is necessary. As a consequence, the security level of micropayment systems may be lower. This may be justified because lower values imply smaller risks. Beside computational costs, efficiency in micropayment systems has further aspects. In more efficient micropayment systems, merchants can request the monetary value from the payer's bank for aggregated micropayments received from one payer by simply presenting one single payment item instead of forwarding every micropayment item. Obviously, such a solution does still not help if a payer spends only some Cents. For such cases, other solutions for cost aggregation are required.

IV.2 Divisibility

For real cash, a payer is either required to have the right denomination, or change will be given to her. In the context of anonymous electronic cash systems, change may be undesired. In contrast to real world cash, divisibility of electronic cash is possible²⁸⁸, i.e., electronic cash can be splitted into smaller values in order to achieve the desired denomination. Thus, a user of a divisible cash system is always able to pay the required amount provided she has enough money. This property can be easily achieved with cheque or credit card payment.

IV.3 Transferability

Traditional cash can be flexibly exchanged among users without the necessity of involving the money issuer. For reasons of cost reduction, flexibility, and usability, users will prefer electronic payment systems that allow transferability of monetary values just as traditional systems do. In electronic payment system literature, transferability is mainly considered for digital cash systems. In most proposed electronic cash systems, cash is only for payments by those parties that have withdrawn them, i.e., transferability is not supported.

²⁸⁷ See: Jakobsson, MRaihi, Tsiounis, Yung (1999); Micali, Rivest (2000).

²⁸⁸ See: Chan, Frankel, Tsiounis (1998); Okamoto, Ohta (1992).

IV.4 Offline Usability

Payment systems should be universally usable, i.e., they should be usable under many circumstances and conditions. This prevents users from being required to deal with multiple payment systems in parallel which may bring some confusion in overviewing their financial status. Thus, even if electronic payment systems are mainly developed to be used for the exchange of monetary values over the Internet, they should also be usable if a payer is not online on the Internet.

IV.5 Financial Status Transparency

In order to plan purchases and economical decisions users appreciate a possibility to have an overview of their financial status. This is easily possible with traditional payment systems by just having a look in the purse or the bank account. Thus, users of electronic payment systems may require a similar property. The possibility for checking the current balance should be given anytime and anywhere. Obviously, it is advantageous if users are able to check their financial status before proceeding to a cash desk. Furthermore, users usually prefer to check their balance privately.

IV.6 Cost Efficiency

Every payment system — both traditional and electronic — produces some overhead costs. Obviously, costs are very important for user acceptance. These costs are caused by many influences which we cannot list here completely. For electronic payment systems these costs may stem from costs for communication networks, for infrastructure and other investments required at banks, merchants and for the payer, e.g., a specific payment device or an electronic wallet, and also fees banks charge for the processing of payments.

V Classification

In general, there are many ways to classify electronic payment systems. In the following, we will consider some aspects according to which one may classify electronic payment systems.

V.1 Online or Offline

Online payment systems involve a third party, e.g., a financial institution, for each payment. This institution usually verifies whether a payment can be accepted, and if yes, then it authorizes the payment. For instance, online verification of digital payments is used for overspending detection, or the payer's solvency. In contrast, offline systems do not require connecting to such a third party, and therefore, they require less communication. Thus, offline systems lower the costs for payments. In an offline system, a merchant can collect payments received over some period of time, e.g., a day, and then forward the collected pay-

ments at once. In general, payments involving larger amounts of money should rather be done by using online systems whereas for lower amounts one could use offline systems.

V.2 Pre-paid, Pay-Now, or Pay-Later

Another aspect of a payment system is the time when the payer's account is debited. In *pre-paid* systems, the account is debited before purchase. This happens in a *withdrawal* phase. Usually, payers do not prefer the pre-paid variant. Pre-paid systems have the disadvantage for payers that they lose potential interests since they have to withdraw money from their account before the payment occurs. In *pay-now* systems, the payer's account is debited at the time of payment. In *pay-later* systems, the merchant's account is already credited at the time of payment, but the payer's account is debited later.

V.3 Hardware-Based or Software-Based

Payment systems can be based on hardware, software, or some kind of hybrid solutions. Hardware-based and software-based systems differ in the way how security is achieved. Hardware-based approaches achieve security by the usage of tamper-resistant hardware^{289,290} The idea of such a hardware is that users cannot manipulate the amount of money they own. Examples for such hardware are smartcards or PDA-like electronic wallets. In principle, software-based systems allow the manipulation of data, but they should prevent that malicious parties obtain any profit out of such manipulations. Thus, software-based systems are usually designed as online payments where a third party verifies the payment whether it is acceptable. There are also hybrid solutions which combine protection means of hardware and software²⁹¹.

V.4 Anonymous or Non-anonymous

The majority of existing systems does not fulfill the confidentiality and privacy requirements we have considered above. If electronic payment systems do not anonymize customers to a sufficient degree, banks are able to collect great amounts of data about their customers. For data mining reasons, this collected information has a considerable value for banks. It can be exploited for own reasons, e.g., discrimination and marketing, or it can be sold to other parties. Anonymous systems prevent this kind of threats. Of course, electronic payment systems cannot prevent information leaks that occur outside the payment system. If payers are interested to protect their personal information then they should decide for an electronic payment system that provides anonymity. Unfortunately, anonymity is usually sacrificed for cost reduction and potential misuse.

²⁸⁹ Note that tamper-resistancy is a strong assumption. Using sophisticated equipment one can attack hardware components

²⁹⁰ See: Anderson, Kuhn (1996).

²⁹¹ See: Brands (1993b).

For the future, there is a need for privacy protecting micropayment systems in order not to lose the important goal of personal data protection.

V.5 In-Band or Out-Band Authorization

Before the bank credits a merchant's account it usually verifies whether the payment is really authorized by the payer. There are several possibilities for the payer to give this authorization to the bank. Thus, some payment systems have a technical method for the provision of such an authorization, e.g., by sending a password or a digital signature to the bank in order to verify that the payer agrees to the payment. Digital signature can provide non-repudiation of the authorization. When the payer's authorization is directly given within the payment system, we call this *in-band* authorization. In other cases, there is no method provided by the electronic payment system itself. Then, we talk of *out-band* authorization. In such systems, the payer can send his authorization on another channel, e.g., authorization via phone, or absence of complaints over a certain period of time is interpreted as authorization. For instance, out-band authorization is used when in-band authorizations over the Internet are assumed to be insecure. On the other hand, out-band authorization may make the payment awkward.

V.6 Cryptography-Based or Cryptoless

Electronic payment systems may apply cryptography or not. Systems which do not use cryptography should not be used for payments over the Internet. Cryptoless systems should involve out-band activities in the payment process. If one can assume a sufficiently high level of security for an authenticated origin then the risk is not too high. However, if the goal is to carry out the whole payment process over the Internet, then one should definitely choose a payment system that applies well-selected cryptographic primitives and protocols.

V.7 Probabilistic or Deterministic

The majority of electronic payment systems employs deterministic methods in all system phases (e.g., withdrawal, payment, deposit). However, there are proposals for electronic payment systems that involve probabilistic methods. The motivation behind this was to reduce costs by increasing the efficiency throughout multiple payments. The application of these techniques was proposed for micropayment systems. In proposed approaches, one can distinguish among the ways according to which probabilistic decisions are applied. These are probabilistic *payment* and probabilistic *verification*. Probabilistic *payment* means that for each payment, the payer and the merchant interact according to a pre-determined process so that with a certain probability a payment is selected, otherwise discarded. In probabilistic *verification* approaches, the merchant initiates a payment verification according to a probabilistic function.

VI Electronic Cheques

A cheque is a payment order addressed to a certain payee and signed by the payer to transfer a certain monetary value from the payer's account to the payee's account. Usually, the payee also signs the cheque and gives it to her bank which takes care of clearing with the bank of the payer. Electronic cheques were assumed to replace the conventional paper-based checks to reduce the processing, transport and communication costs. Basically, an online verification must be done in a purchase to ensure that the underlying cheque is backed. However, to reduce the communication overhead an offline verification would be sufficient. In the following, we present some proposals for electronic cheque systems.

An electronic cheque architecture was designed and implemented by the *Financial Services Technology Consortium* (FTSC)²⁹². This system requires that authorized users obtain a smart-card based electronic chequebook device which is assumed to be tamper-resistant. This device stores information such as signing key and certificates and has the role of an observer taking care of the cheques that have been issued previously. The payee should possess a similar device. After the payee forwards the cheque to his bank, the financial network takes care of authorization and clearing.

Another electronic cheque system is contained in the *NetBill* system²⁹³. It intends to provide a complete trading system from the *negotiation* phase to the *delivery* of goods. In the negotiation phase, the buyer and the merchant agree upon terms and conditions. For the buyer to be able to obtain the good, the merchant must verify the validity of the cheque where a third party, the *NetBill* server, is involved in the payment. *NetBill* payments require mutual identification of the involved parties. This procedure is based on a modified version of *Kerberos*²⁹⁴, i.e., to use public key cryptography on the top of symmetric cryptography.²⁹⁵ Another online cheque-like system also based on *Kerberos* is *NetCheque*²⁹⁶.

One of the properties of common cheque systems is their auditability, i.e., they allow banks to identify payers and payees. Unfortunately, this property is in contradiction with the requirement concerning privacy protection, since it allows a bank to monitor the spending patterns of the payer.

VII Credit Card Payments

Payment systems based on credit cards are widely established payment methods, and have been in use for many years. In reality, one can distinguish between credit card associations and banks. However, for the sake of simplicity, we call them banks. In a purchase, the merchant asks the payer for card information (e.g., number, expiry date), and depending on his policy, the payment may be

²⁹² See: Anderson (1998).

²⁹³ See: Sirbu, Tygar (1995).

²⁹⁴ See: Steiner, Neuman, Schiller (1988).

completed at this point, or the merchant makes an online verification with the bank regarding the payer's solvency.

To be able to transport purchase and credit card information in a secure and authentic way over the Internet, the payer and the merchant can apply cryptographic protocols such as *Secure Socket Layer (SSL)*²⁹⁵. The IETF has adopted the *SSL* protocol and renamed it to *Transport Layer Security (TLS)*. This protocol is widely used for credit card payments in practice, however, it is no payment system. This protocol is rather a standard that provides secure channels and data authentication for *http* communication. The driving idea for the development of the *SSL* protocol was to secure the transmission of credit card numbers. This protocol allows an authentication of the merchant server (payer authentication is optional) after which a secure communication channel is established between the payer and the merchant, i.e., all messages are encrypted. However, protocols like *TLS* cannot take care of other issues required for electronic commerce transactions, e.g., for verifying the validity of the credit card, authorizing the payment, and interaction with clearing processes. Another problem is that the merchant is not prevented from accessing and misusing purchase information (e.g., card information). Moreover, it does not provide non-repudiation against cheating parties. Note that this requirement is crucial for promoting trade over the Internet. Nevertheless, *SSL/TLS* is widely used today for credit card payments over the Internet.

In parallel to this, more specific credit card systems for Internet payments have been developed which were not successful at the market. For instance, there have been *First Virtual* and *CyberCash*. *First Virtual* was shut down in 1998. It satisfied a minimum level of security by password authorization for payments, but did not apply cryptographic techniques. *CyberCash* credit card payment²⁹⁶ was contained in a comprehensive concept integrating distinct types of Internet payments. It applied public key cryptography which provided higher level protection for purchase data and authorization reasons.

Another development to be mentioned here is *i-Key Protocol (iKP)*²⁹⁷. Historically, it is an important system for further developments in this area, even if it is not used in real world applications. The models of *iKP* involve a third party acting as a payment gateway between the users of the system and the existing financial network. The main role of this gateway is to authorize the payment. During a purchase, the merchant sends the purchase data (e.g., credit card number, etc.), he obtained from the payer, to the gateway which forwards this information to the bank network where it is decided whether to authorize the payment. The result is sent back to the merchant through the gateway. The

²⁹⁵ *Kerberos* is a trusted third party authentication service enabling servers in an open distributed environment to control access and to authenticate requests for services.

²⁹⁴ See: Neuman, Medvinsky (1995).

²⁹⁵ See: Dierks, Allen (1999); Freier, Karlton, Kocher (1996).

²⁹⁶ See: Eastlake, Boesch, Crocker, Yesil (1996).

²⁹⁷ See: Bellare, et al. (1995); Bellare, et al. (2000).

payment system iKP ($i = 1, 2, 3$) represents a family of payment systems where i indicates the number of parties who possess an own key pair. For instance, in $3KP$ all involved parties, i.e., the payer, the merchant and the gateway have private / secret key pairs whereas in $2KP$ the buyer is the only one without own key pair. Individual protocols differ in both complexity and degree of security. To deal with non-repudiation, each of the involved parties (payer, merchant and gateway) can generate digital signatures. To protect payer's sensitive information from the merchant, all messages from the payer to the gateway via the merchant are encrypted with the gateway's public key.

iKP is a precursor of the well-known *Secure Electronic Transaction (SET)* standard²⁹⁸. The *SET* protocol was jointly developed by a consortium of credit card associations, among others. It enhances the earlier protocols by improving the cryptographic protection mechanisms for purchase details and allowing to use a certification authority hierarchy.²⁹⁹ From the today's perspective, it can be stated that the high expectations concerning the deployment of *SET* have not been fulfilled. Now, some remarks are in place.

- As mentioned before, iKP and *SET* use digital signatures to authenticate messages and authorize transactions where these digital signatures should make the parties' authorizations non-repudiable, i.e., provable to a third party. However, one has to take care of which kind of statements which participants in a payment may want to prove and can prove, and what are the requirements for provability in payment protocols³⁰⁰.
- Payment protocols with features as offered by *SET* are computationally costly since they require to carry out quite a number of expensive computations such as of digital signatures. Moreover, such systems operate *online* involving a third party payment gateway for the purpose of authorization and clearing. However, this leads to additional communication overhead. Note that the offline version would reduce this, however, it cannot prevent the misuse of card information.
- The mentioned credit card schemes do not protect the privacy of the payer since banks can identify the payer and monitor payer's commercial relationships, e.g., on card information or her signature verification key. In order to protect the payer's privacy against collecting behavioristic profiles, some solutions have been proposed to make credit card transactions anonymous³⁰¹. However, the anonymity can be revoked if several parties collude and compare the transcripts of payment processes. To our knowledge, these proposals are not applied in real world solutions.
- Today, credit cards are often used for Internet payments. They also have some advantages to be used in international commercial relationships where other systems like cheques, remittance, or debit order payments are rather

²⁹⁸ See: SET (1997a/b/c).

²⁹⁹ A certification authority is an infrastructure component that certifies public keys of the involved parties such as cardholders, merchants, banks.

³⁰⁰ See: Herreweghen (1996/2000).

³⁰¹ See: Low, Maxemchuk, Paul (1994).

unsuitable, e.g., due to high overhead costs. The costs for one credit card payment are currently in the range of about 20 – 40 Cents, with a little extra charge if they are used in a international context. Thus, they cannot be used for low-value payments.

VIII Cash Systems

Electronic cash is broadly defined as electronically stored monetary value³⁰². It intends to realize real world cash in an electronic way exploiting the merits of digital technologies. Nevertheless, electronic cash is often debated as a replacement for conventional cash, in particular, because it is expected to be less costly. Internationally, there have been many trials to introduce electronic cash products into the market, e.g. see CPSS BIS³⁰³. For electronic cash to really replace traditional cash, however, it should provide typical properties such as offline usability, privacy (pseudonymity, unlinkability), transferability and unforgeability (see Sections III and IV and also Schmidt, Schunter, Weber³⁰⁴, or CPSS BIS³⁰⁵). Unfortunately, until now there is no electronic cash system capable of satisfying all these requirements.

Over the past years a large number of electronic cash systems have been proposed offering different security levels and properties. In particular, designing *anonymous cash systems* has attracted many researchers. Most of these proposals offer only *payer anonymity* and only in the *payment phase*, but with *unlinkability*, i.e., the merchant, bank or their collusion cannot link a payment to the corresponding withdrawal.

The best-known systems in this class apply a cryptographic primitive called *blind signatures* to implement anonymity. These systems are also called *coin systems* on which we will mainly focus in the following.

The ingenious concept of *blind signatures* was introduced by Chaum³⁰⁶. Other than a normal signature, a blind signature is issued by an interactive protocol between a signer and a receiver. At completion of this interaction, the receiver obtains a signature on the message to be signed while the signer knows neither the message nor the signature on it. Loosely speaking, the goal is to prevent the signer from relating a signature, it observes later, to the receiver. This is called *blindness* requirement.³⁰⁷ At first glance, the idea of blind signatures sounds odd, however, it can be employed for constructing privacy protecting cryptographic

³⁰² See: CPSS BIS (1996).

³⁰³ See: CPSS BIS (2000).

³⁰⁴ See: Schmidt, Schunter, Weber (1998).

³⁰⁵ See: CPSS BIS (1996).

³⁰⁶ See: Chaum (1983/1984/1985).

³⁰⁷ More precisely, blindness means that given a set of transcripts of the blind signature protocol-runs, and the set of message-signature pairs generated by these protocol-runs, the signer cannot associate the protocol-runs with the message-signature pairs with a probability significantly better than pure guessing.

applications such as anonymous electronic cash. The basic idea is illustrated in Figure 2 and described in the following.

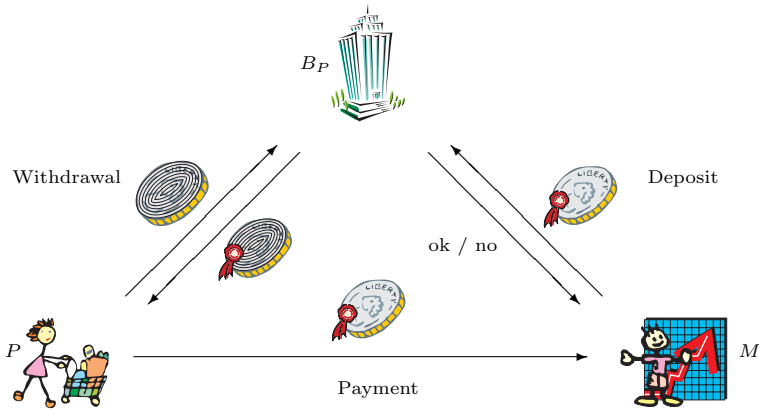


Fig. 2. Blinding of Digital Coins

During withdrawal, the payer P generates a coin c . The bank as the issuer of electronic coins signs these using a blind signature. This means, P blinds c by applying an appropriate transformation. We denote the blinded coin with c' , which is depicted by the shaded coin in Figure 2. P sends the blinded coin c' to the bank B together with a withdrawal order. This order contains mainly information about P 's account and the amount of money she wants to withdraw for this coin, e.g., 1 Euro. The bank B debits P 's account by the corresponding amount and signs c' with a signing key of a special public key pair which indicates c 's value. We denote the resulting signature with σ' .

During payment, P unblinds the signature σ' to a signature σ which corresponds to the unblinded coin c . P sends the pair (c, σ) to M who verifies the signature with the verification key of the bank.

During deposit, B verifies the validity of the coin by verifying σ , and verifies against double-spending, i.e., it searches in its database whether this coin has been deposited before. If both verifications are true, B accepts the coin, deposits the corresponding value to M 's account, and sends the result to M . If M agrees, he may sign a receipt for P .

Note that we restrict our considerations to the basic principles common to most cash systems. However, for secure and real life application, one requires further measures.³⁰⁸

An important security requirement on cash systems is *double-spender identification*. This is a mechanism which allows the bank to link double-spent cash to the

³⁰⁸ For instance measures to provide secure dispute handling between the involved parties. Disputes may arise when a party claims that its statement of account is not correct, or the bank considers a coin as double-spent, but, the payer claims the opposite (see Pfützmann, Waidner, Pfützmann (1987/2000) for a comprehensive discussion).

withdrawal of a payer and consequently identify this payer. This problem is less important in case of online systems since the bank is involved in each payment. In this case, the bank maintains a database with all spent cash, and immediately verifies whether it is doublespent. Doublespender identification in offline systems is more involved since the bank can detect it after the fact. One solution is to implement an electronic *wallet with observer*, a hardware device which can prevent from any copy or modification attempts. However, this solution requires tamper-resistance.

Most proposed solutions construct cash systems in such a way that the identity of the user is known, and any double-spending attempt would lead to identification after the fact. To realize this without sacrificing the anonymity, advanced cryptographic techniques are applied. The desired mechanisms must exploit the fact that two deposits with the same coin reveal the information required for the purpose of identification, but, this must be infeasible with a single payment. One way to implement this is to use the *challenge and response* principle as proposed in Chaum, Fiat, Naor³⁰⁹ for the first time. There, in each payment, the receiver challenges the payer by asking a question. The payer has to correctly answer by sending a response. There are different ways proposed to realize this³¹⁰. For this, the payer secretly encodes her identity into the coin during the withdrawal to be verified by the bank. The payer remains anonymous as long as there is a single response in the payment for a coin. However, a further payment with the *same* coin will generate a second response, and the bank can use the two different challenges and responses to recover the encoded identity later at deposit.

Since Chaum's publication of blind signature and its deployment for constructing electronic coin systems, there have been many proposals for such systems, particularly offline systems³¹¹. They differ in their underlying cryptographic systems, the properties they offer, and their efficiency.

Electronic coin systems mentioned before are not transferable since a coin can only be spent once before depositing it. For a coin to be transferable, it must also contain the blinded identifying information about all its owners. This means, however, that the coin grows in size³¹².

In the past, there have been some achievements to implement electronic cash systems. Here, we will mention a few of them:

- A well-known product for a coin system is *ecash* conducted by DigiCash. It realizes an online coin system with payer anonymity and non-anonymous accounts based on the ideas of David Chaum³¹³.

³⁰⁹ See: Chaum, Fiat, Naor (1990).

³¹⁰ See: Franklin, Yung (1993); Brands (1993b).

³¹¹ See: Okamoto, Ohta (1990); Ferguson (1993); Brands (1993a/b); Brands (1995); Okamoto (1995).

³¹² See: Chaum, Pedersen (1993a).

³¹³ See: Chaum (1984/1985/1989).

- One of the most efficient offline coin systems is proposed in Brands³¹⁴. It is based on the blind signature scheme introduced in Chaum, Pedersen³¹⁵, and offers unconditional payer anonymity. An European research project on developing anonymous offline electronic cash was *CAFE* (Conditional Access for Europe).
- Another example for an electronic cash system is *NetCash*³¹⁶. *NetCash* is an online payment system using identified coins, i.e., coins are tokens with serial numbers signed by the bank. It uses symmetric and asymmetric cryptography to establish secure channels. Since *NetCash* uses identified coins, it cannot provide anonymity, at least not to the degree as other coin systems provide.
- *Mondex* is a smart card based solution for which most technical information was not published. Users load their cards at *Mondex* ATMs. For payments the money is transferred from one card to another through an appropriate device and no online verification with the bank is needed.

IX Escrowed Cash Systems

Anonymous cash systems have also a dark side. The anonymity property can be misused for illegal transactions and criminal activities such as blackmailing and money laundry (see also Froomkin/ Sander, Ta-Shma³¹⁷). This was first addressed by Solms, Naccache³¹⁸ where they consider the problem of blackmailing the bank also known as *blindfolding*. Since then effort has been put into designing *anonymity-revocable* payment systems, also called *fair* or *escrowed* cash systems³¹⁹. In such systems, one or more trusted third parties (called trustees) can help the bank to revoke the anonymity, in case of justified suspicion.³²⁰ A well-structured survey on such systems can be found in Petersen, Poupard³²¹. The role of the trustee can be *active* or *passive*. An active trustee is involved in registration (opening an account) or in every withdrawal protocol, or even in payment. Systems with passive trustees³²² are more practicable, since the trustee

³¹⁴ See: Brands (1993a).

³¹⁵ See: Chaum, Pedersen (1993a).

³¹⁶ See: Medvinsky, Neuman (1993).

³¹⁷ See: Froomkin (1996); Sander, Ta-Shma (1999).

³¹⁸ See: Solms, Naccache (1992).

³¹⁹ See: Brickell, Gemmell, Kravitz (1995); Camenisch, Maurer, Stadler (1996); Camenisch, Maurer, Stadler (1997); Camenisch, Piveteau, Stadler (1996); Davida, Frankel, Tsiounis, Yung (1997); Frankel, Tsiounis, Yung (1996/1998); Jakobsson, Yung (1996); Solages, Traoré (1999).

³²⁰ For instance, the specific mechanism applied against user blackmailing is *coin tracing*. It is similar to tracing serial numbers of banknotes. The trustee is given specific withdrawal transcripts which the bank has stored during the withdrawal protocol. The trustee is asked to retrieve information to be used by the bank or the merchant to recognize the spent coins. This helps the authorities to find the destination of the extorted money.

³²¹ See: Petersen, Poupard (1997).

³²² See: Camenisch, Maurer, Stadler (1996); Davida, Frankel, Tsiounis, Yung (1997); Frankel, Tsiounis, Yung (1996/1998); Solages, Traoré (1999).

is not involved in any of the system's protocols. The trustee is present passively through its public and authentic parameter (e.g., public key). The common approach is that the payer encrypts some information using the trustee's public key and proves to the bank — and in some approaches to the merchant — that the content of the encryption or a transformation of it will appear in the coin, and thus, reveals the required tracing information. However, for a large class of existing proposals for anonymity–revocable cash the problem of a blackmailing user can be solved without involving any trustee^{323, 324}. Note that the mentioned proposals cannot prevent blindfolding protocols. Examples of systems with mechanisms against such attacks are Fujisaki, Okamoto/ Jakobsson, Yung/ Petersen, Poupard³²⁵.

An alternative but rather inefficient approach for designing anonymous electronic cash systems with tracing capabilities is introduced in Sander, Ta-Shma³²⁶. It is an auditable system and requires no blind signatures. The security of the system relies on the ability of the bank to maintain the integrity of a public database.

X Micropayment Systems

With the rapid growth of open communication networks, they will be increasingly used for delivering low-valued (e.g., less than 1 Cent) information goods and services to a large number of consumers. Examples for such applications are browsing web pages of online magazines and newspapers, querying databases, downloading music or video streams, among others. Most of the previously presented electronic payment systems are not really adequate for handling micropayments due to their high processing costs, e.g., because of computational and communication overhead.

Some of the proposed micropayment systems have already been tested in practice, but so far, they did not achieve a broad market acceptance. The experiences made so far may be valuable for the development of new successor generations of micropayment systems.

The model of some micropayment systems involves an additional party called *broker*. A broker can be considered as an intermediary among payer, merchant, and banks. It is used for functional purposes, e.g., to introduce flexibility for payers by exchanging merchant-specific currencies or by allowing them to be in contact with many merchants without being required to open accounts at each merchant. For the sake of simplicity, we consider brokers to belong to the financial infrastructure. Thus, we do not differentiate brokers from banks.

³²³ See: Pfitzmann, Sadeghi (2000).

³²⁴ More concretely, instead of a trustee, the blackmailed person herself reveals the required information to trace extorted coins without compromising any of her secrets.

³²⁵ See: Fujisaki, Okamoto (1997); Jakobsson, Yung (1996/1997); Petersen, Poupard (1997).

³²⁶ See: Sander, Ta-Shma (1999).

There is a relatively large body of literature on micropayment systems. As mentioned before, these systems do not offer all desired properties (e.g., anonymity) of some electronic macropayment systems. Well-structured categorization and analysis of many of these systems are given in Lipton, Ostrovsky/ Peirce/ Weber³²⁷. Here, we categorize micropayment systems according to their property whether transactions in payment systems are either dependent on some probabilistic decisions (see Section V).

X.1 Payment Transactions without Probabilistic Decisions

Here, we consider those micropayment systems whose execution is not dependent on the outcome of random experiments. The systems to be considered here can be distinguished according to the degree they use costly computations, mostly resulting from cryptographic computations. Certain categories of cryptographic primitives (symmetric cryptography, asymmetric cryptography) cause different costs.

A system which can operate with very little cryptography is *MilliCent*. *MilliCent* is a micropayment system which uses special forms of electronic coins called *scrip*³²⁸. Scrip can be understood to be similar to a pre-paid calling card, or a debit card specific to a merchant. Scrips are merchant specific, i.e., they can only be spent at their corresponding merchants. Payers can buy larger amounts of scrip in a single transaction by using an appropriate macropayment system. The bank maintains accounts of payers and merchants. The main security problem of this type of micropayment schemes is overspending, and proposed measures such as online verification, or maintaining blacklists about cheating users by all concerned merchants and banks are expensive. *MilliCent* offers three different protection levels. The strongest protection level applies symmetric cryptography with scrip-based exchange of a shared key for the provision of security, e.g., to deal with scrip forgery and privacy in communication. The second level does not use symmetric cryptography whereas the lowest level provides no security at all.

There are other systems reducing computational effort by exclusively using symmetric cryptography in order to allow small-value transactions. In these systems, symmetric cryptography is mainly used for purposes such as authentication and authorization of fund transfers between the payer's and the merchant's account, i.e., the payer authorizes the payment order by using the secret key which she shares with the bank. Since the merchant does not know the secret key of the buyer, he is not able to forge purchase details or to obtain information since it is exchanged in an encrypted way. Here, the payment order is just an instruction for the bank to debit the payer's account. Note that in these systems no coin-like monetary values are used or stored, and therefore, no overspending is possible. As mentioned before, these systems are online and are inefficient if used frequently. Examples are the online payment system of Tang³²⁹ and *Cyber-*

³²⁷ See: Lipton, Ostrovsky (1998); Peirce (2000); Weber (1998).

³²⁸ See: Glassman, Manasse, Abadi, Gauthier, Sobalvarro (1995).

³²⁹ See: Tang (1995).

Coin which was developed as an extension to *CyberCash* (see O'Mahony, Peirce, Tewari³³⁰). Another advantage of such systems is that payer system crashes do not result in monetary loss for her. Unfortunately, the payer's privacy is not protected since the bank gets aware of the payer's commercial relationships.

Other payment schemes allowing small- and low-value payments use asymmetric cryptography, e.g., to generate digital signatures, even if this requires higher computational effort. These systems use asymmetric primitives for payer authentication and payment authorization. Examples for such systems are *NetBill* (see Section VI) and *NetCent*³³¹. *NetCent* improves *MilliCent* mainly in the sense that *NetCent* scrips are not merchant specific and can be directly transferred from one merchant to another. Overspending is not possible since the payment order is just an instruction for crediting the payer's account by subtracting the corresponding amount from the current balance.

MiniPay is another micropayment system which applies asymmetric cryptography with its focus on web applications. It allows to "pay a Cent per click"³³². The idea of *MiniPay* is to save costs for payment order transmission by attaching it on the payer's *http* information request (GetURL). It is proposed that the typical bank's part are played by an Internet service provider and an Internet access provider. Each payment order sent to the merchant is signed by the payer. Payments will be accepted if they are within a given monetary range valid for a specific period of time, e.g., a day. This limit is contained in the payer's public key certificate. Merchants collect the payments obtained from their customers before they forward them for deposit reasons in an aggregated way. While collecting, no verification other than that of signatures is performed. This reduces communication costs as they usually arise in online payment systems. On the other hand, this allows overspending; it is possible that a payer spends money up to its limit at many merchants within the corresponding period. Furthermore, all signatures generated by the payer have to be transferred and verified for deposit which entails costs for communication and computation. Another system similar to *MiniPay* was proposed in Blaze, Ioannidis, Keromytis³³³.

There are micropayment systems in which merchants do not need to forward all collected payments to the bank, though, they allow the bank to implicitly verify all the payments at deposit. A class of micropayment systems providing this property is based on *one-way chains*.³³⁴ The first proposal for such a payment system was given in Pedersen³³⁵. The basic idea is to implement micropayments with a one-way chain introduced in Lamport³³⁶. Let f be a one-way

³³⁰ See: O'Mahony, Peirce, Tewari (1997).

³³¹ See: Poutanen, Hinton, Stumm (1998).

³³² See: Herzberg, Yochai (1997).

³³³ See: Blaze, Ioannidis, Keromytis (2001).

³³⁴ These systems are also called *coupon-based* systems.

³³⁵ See: Pedersen (1997).

³³⁶ See: Lamport (1981).

function (e.g., a secure one-way hash function).³³⁷ The payer computes the value $w_n := f^n(w_0)$ where w_0 is a random value, and f^n denotes n iterations of the function f , i.e., $w_0 = f^0(w_0), w_1 := f(w_0), w_2 := f(w_1) = f^2(w_0), \dots, w_n = f^n(w_0)$. The chain elements w_i are used by the payer to make micropayments of a fixed value v . As an example, consider a payer sending subsequently $n = 10$ chain elements to the same merchant where each element has a value of 1 Cent, she gives him a total value of 0.1 Euro. Before starting the payments, the payer commits to the entire chain by signing the last element w_n of the chain and sends it to the merchant.³³⁸ After the merchant has verified the signature, each successive payment is carried out by revealing $w_{n-i} := f^{n-i}(w_0)$ for the i -th payment to the merchant, i.e., the chain of hash values is spent in reverse to the way it was generated. The merchant stores the payer's signature on w_n and also the last obtained value w_{i-1} to be able to verify the next micropayment w_i . To clear the payments, the merchant presents the signature on w_n and the last obtained chain element w_{n-k} for $(0 < k \leq n)$ to the bank. Note that beside the signature on w_n , only one chain element has to be transferred to the bank. The bank can re-calculate the relevant part of the initially generated hash value chain and verifies whether $f^k(w_{n-k}) = w_n$ holds. After positive test, the bank credits the merchant k times the value of a chain element, e.g., k Cents. Other similar coupon-based micropayment systems with hash chains are *PayWord*³³⁹, *micro-iKP*³⁴⁰, *NetCard*³⁴¹ and *PayTree*³⁴².

A further scheme based on a specific form of electronic coins is *MicroMint*³⁴³. *MicroMint* coins can be spent at any merchant. In the model, the coins are minted by a bank and sold to the payers. After a payment, coins are redeemed to the bank by merchants. In contrast to other electronic macropayments, coins do not represent the signature of the bank on a value since signing and verifying a coin would be computationally expensive. Instead, they propose a method for minting and verifying coins based on n -collisions of one-way hash functions.³⁴⁴ To be able to mint and verify coins efficiently, the authors propose that the bank must be provided with special-purpose hardware devices to be able

³³⁷ Informally, a function from a set X to a set Y is called one-way function if $y := f(x)$ can be computed efficiently but it is infeasible to compute x from y .

³³⁸ The payer may also sign other data such as the value of a chain element, the merchant's name, or a sequence number to avoid replay attacks.

³³⁹ See: Rivest, Shamir (1997).

³⁴⁰ See: Hauser, Steiner, Waidner (1996).

³⁴¹ See: Anderson, Manifavas, Sutherland (1997).

³⁴² See: Jutla, Yung (1996).

³⁴³ See: Burstein (1998); Rivest, Shamir (1997).

³⁴⁴ More precisely, a coin is a n -way hash function collision. Let f be a one-way function. An n -collision occurs, if there exist n different values x_1, x_2, \dots, x_n which are mapped to the same value by the function f , i.e., $f(x_1) = f(x_2) = \dots = f(x_n) = y$. A coin will then be (x_1, x_2, \dots, x_n) . However, finding such collisions is computationally not easy. Note that f cannot be implemented by usual one-way hash functions, e.g., MD5 or SHA-1. For those it is assumed that finding collisions is infeasible.

to perform the hashing required for minting coins, i.e., finding collisions. Such hardware and several other measures are required to prevent large-scale forging of coins. Moreover, the scheme offers no means against doublespending and can only use blacklisting offenders by keeping track of overspent coins from payers and merchants.

X.2 Payment Transactions with Probabilistic Decisions

As we have seen in previous sections, electronic (micro)payment systems are either online and involve a third party in each transaction for verification against overspending, or they are offline and can detect overspending after the fact. To reduce the number of transactions, a new class of micropayment systems based on *probabilistic decisions* has been introduced. In this context, there have been two different approaches, namely, probabilistic *verification* and probabilistic *payment*. Examples for the former approach are *probabilistic audit*³⁴⁵ and *probabilistic polling*³⁴⁶. The basic idea is that at purchase the payer gives signed payment orders to the merchant who decides only with a certain — rather small — *probability* to contact the third party (e.g., bank) for payment verification. The decision probability may be constant³⁴⁷ or proportional to the amount of the payment³⁴⁸. This idea combines the methods of online and offline payment systems to limit overspending while eliminating the need for verifying each payment. The shortcoming of these schemes is that doublespenders must be blacklisted, and all merchants must be informed and a revocation list must be maintained either at the merchants or at the bank. Another proposal using randomized audit in combination with hardware is given in Yacobi³⁴⁹. Also here, compromised smart cards must be revoked and the revocation list must be broadcasted to all merchants.

Next, we consider the probabilistic payment approach. One of the first proposals is given in Wheeler³⁵⁰. The basic idea is that for each micropayment the payer and the merchant interact according to a pre-determined protocol, e.g., the coin flipping protocol in Blum³⁵¹, so that with a small probability p this micropayment is selected, otherwise discarded. In other words, for each payment the payer has to pay a larger amount with probability p , and with probability $1 - p$, the payer pays nothing. For instance, if $p = 1/1000$ and the value of a micropayment should be 0.1 Cent, then, out of 1000 micropayments 999 will be discarded and 1 will be paid for 100 Cents on average. The advantage of this approach is that the bank requires to process only one single payment. Based on the ideas

³⁴⁵ See: Gabber, Silberschatz (1996).

³⁴⁶ See: Jarecki, Odlyzko (1997).

³⁴⁷ See: Gabber, Silberschatz (1996).

³⁴⁸ See: Jarecki, Odlyzko (1997).

³⁴⁹ See: Yacobi (1997).

³⁵⁰ See: Wheeler (1997).

³⁵¹ See: Blum (1982).

in Wheeler³⁵², Rivest proposes a lottery ticket based micropayment scheme³⁵³. The basic idea is that the payer issues a signed lottery ticket containing a *ticket value* and a *winning value* used later to determine the winner.³⁵⁴ If the payer has used the winning ticket and has given it to the merchant then he will be charged, otherwise not. A specialization using two hash chains is proposed in Rivest³⁵⁵ which avoids the usage of digital signatures. Some of the main shortcomings of this system type are (i) the payer is not bound to the outcome of the coin flipping protocol, and thus, can refuse to pay if the outcome is not in her interest, and (ii), no solution is proposed for the case the protocol is aborted at some stage which is known as the *fairness* aspect. Note that if this is allowed, then any of the involved parties may abort and restart the coin-flipping protocol changing the probabilities to its advantage. The payment system in Lipton, Ostrovsky³⁵⁶ uses the ideas in these papers and proposes solutions to the mentioned problems. More precisely, they present an authenticated coin-flipping protocol and prove its security. However, to achieve provable security they need to apply computationally expensive *zero-knowledge proof of knowledge protocols* where the user (merchant) proves to the merchant (user) that she (he) knows a certain value.³⁵⁷

Other probabilistic micropayment systems retaining the ideas of lottery tickets and *PayWord* are proposed in Micali, Rivest³⁵⁸. The authors address the main problems of micropayment systems such as *PayWord* and *Lottery Tickets* concerning efficiency and security, and propose solutions to remedy these shortcomings³⁵⁸. The main efficiency problem of *PayWord* is that the merchant cannot aggregate the micropayments of different users, i.e., the bank must also deposit a single micropayment which is not really viable due to the processing cost. The efficiency problem of *Lottery Tickets* relies in the interaction between the user and the merchant for selecting the micropayment. Moreover, in this scheme the payer has the risk that she may pay more than she should due to the probabilistic decision.³⁵⁹

³⁵² See: Wheeler (1997).

³⁵³ See: Rivest (1997).

³⁵⁴ The winning value can be a commitment, e.g., $y := h(x)$ where h is a secure hash function, to a value x which the payer should not learn at the time she issues the ticket. The commitment should be supplied by another party. The receiver has to know x in order to determine whether he is in possession of a winning ticket. In a concrete system, the merchant generates x , e.g., the outcome of an online coin-flip, and supplies the payer with y .

³⁵⁵ See: Rivest (1997).

³⁵⁶ See: Lipton, Ostrovsky (1998).

³⁵⁷ Loosely speaking, in a zero-knowledge proof of knowledge a prover proves to a verifier that she knows a secret value without revealing any information about this value.

³⁵⁸ See: Micali, Rivest (2002).

³⁵⁹ Note that although due to the law of large numbers the probability of such an event is small, the authors mention that this risk might have a great impact on the acceptance of such payment systems.

XI Past and Today's Practice

Many activities for establishing electronic payment systems into the market have been pushed by financial institutions and organizations. Thus, the availability of products has been mostly geographically bound due their spheres of activity. Many systems, which have been introduced, have already disappeared or have only reached a limited number of users. Furthermore, there is a considerable dynamic in this market. So, the situation may change between the time of this writing and publishing.

Here, we will restrict our considerations only to a small fraction of those systems which have been implemented as products — either still in use or presently not available anymore. Future needs concerning the availability of payment systems may bring some practical solutions back into the game. More information concerning various electronic payment systems can be found at <http://www.ex.ac.uk/~RDavies>.

DigiCash's product *ecash* was used by the American *Mark Twain Bank*, the Finish *Eunet*, and by *Deutsche Bank*, Germany, among some others. It was a pre-paid coin system based on *Chaum's* idea³⁶⁰. However, field trials with this system have been stopped, and the payment system is not provided anymore.

In the late 90s, *MasterCard* and *Visa* started to try pushing *SET* as an electronic credit card system into the market. Even if it promised better protection than sending credit card numbers over secured connections, *SET* was not really successful. Implementation and usage were too expensive for many merchants and payers.

PayPal is a rather successful payment system which allows person-to-person payments which became very popular. According to Punch³⁶¹, there have been more than 10 Millions of *PayPal* users in the United States in year 2001. This success is strongly related to its deployment in the *eBay* online auction system which became very popular. The auction business model exactly requires the person-to-person functionality that *PayPal* provides. Payer and payee have accounts at the *PayPal* provider. Payments are sent via emails. The payer sends an email to the provider and gives him the email address of the payee. Then, corresponding accounts are debited and credited. In the background, an ordinary credit card payment system is used for transferring money between a user's bank account and his *PayPal* account.

Paybox is a pay-now system that uses out-band authorization to authorize the payment. In the *Paybox* system, the authorization is given via a mobile phone, and thus it is not sent via the Internet. In a purchase, the payer sends his mobile phone number to the merchant who forwards this number together with the payment amount to the *Paybox* provider. Afterwards, the provider calls the payer in order to let her authorize the payment. The payer is authenticated by possession of the mobile phone and by typing-in some additional secret. After

³⁶⁰ See: Chaum (1983/1989).

³⁶¹ See: Punch (2001).

positive authorization, the *Paybox* provider requests the corresponding amount from the payer's account via a *debit order* payment system. Obviously, *Paybox* requires a mobile device, e.g., a mobile phone which has extremely high diffusion today. The provider at least learns about the relationship among payers and merchants, and also how much a payer spends at merchants.

XII Conclusion

In this work, we have given a survey on electronic payment systems. In the last years, there have been many proposals for electronic payment systems both in the industrial and academic area. However, many attempts to push these into the market unfortunately failed so far, but for their future, some conditions may change. Electronic payment systems seem to be promising in the future, especially those systems that allow payments over networks. When commerce with digital goods delivered over the Internet will evolve then secure electronic payment systems will become more and more relevant. New future applications in the area of information commerce, stimulated by the developments in digital rights management systems, will require comfortable and immediate payments. Many electronic payment systems as they are proposed by the academic community are still not applied and implemented in current products, although they provide users with much better security and privacy properties than systems that are often used today. In the past, lots of proposals have been criticized due to their inefficiency, but with the development of more powerful computer systems and networks these requirements become less dominating. Payment systems used today also consider security to some extent but they widely neglect privacy aspects. However, in practice providers promote their payment products by praising their security properties. Unfortunately, most customers are not really able to compare these products on their own by the information they are given.

Since the deployment of electronic payment products heavily depends on financial institutions and organizations focusing on national markets, there has been a lack of coordinated activities at an international level in this area so far. However, experiences made will be valuable for future decisions and developments.

From the today's perspective, there seems to be no question that electronic payment systems will evolve. Unfortunately, it is still impossible to say which system will be the future standard Internet payment system. Finally, this question will be answered by banks, merchants, governments, and also by the mass of normal users.

XIII Acknowledgement

We are grateful to M. Fuckard for many valuable comments and for his infinite readiness to help. Also many thanks to Michael Steiner for his valuable hints and for his efficient cooperation.